REMARKS

Claims 1-47 are pending in the application. Claims 1-47 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Risks of the Passport Single Signon Protocol by David P. Kormann and Aviel D. Rubin, published in Computer Networks 33, pages 51-58 (June 2000) ("Kormann"). Claims 1-47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Windows 2000 Authentication (http://www.comptechdoc.org/os/windows/win2k/win2kauthentication.html) ("Comptech Article").

Reconsideration is requested. The rejections are traversed. No new matter is added. Claim 19 is amended. Claim 48 is added. Claims 1-48 remain in the case for consideration.

The Applicant thanks the Examiner for explaining why claim 47 is considered rejected under 35 U.S.C. § 103(a) over "Comptech Article".

The Applicant objects to the Examiner's rejection of the claims under 35 U.S.C. § 102(e). 35 U.S.C. § 102(e) only applies if the reference in question is a published patent application that was filed before the filing date of the patent application, or if the reference is an issued patent that was filed before the filing date of the patent application. Kormann is neither a published patent application nor an issued patent. Accordingly, the proper rejection of the claims should be under 35 U.S.C. § 102(a). The Applicant treats the claims as rejected under 35 U.S.C. § 102(a).

RESPONSE TO ARGUMENTS REGARDING THE INAPPLICABILITY OF "COMPTECH ARTICLE" USED IN THE REJECTION UNDER 35 U.S.C. § 103(a)

In the Office Action dated February 26, 2007, the Examiner states that "[e]ven, assuming arguendo, that Applicant is correct regarding the inapplicability of the Windows 2000 reference ["Comptech Article"] (used in the rejection under 35 U.S.C. § 103), Applicant's arguments are moot in view of the new ground(s) of rejection with the Kormann reference. See the rejection under 35 U.S.C. § 102" (*see* Office Action dated February 26, 2007, page 2; emphasis in original).

The Applicant respectfully disagrees that the Applicant's arguments are moot. While the Applicant agrees that the rejection under 35 U.S.C. § 102(a) relies on a reference other than "Comptech Article", the Examiner continues to maintain the rejection under 35 U.S.C. § 103(a), rejecting claims 1-47 as obvious over "Comptech Article". For example, if the rejection of the

claims under 35 U.S.C. § 102 over Kormann should prove to be inappropriate (as argued below), then the rejection of the claims under 35 U.S.C. § 103(a) would once again be the only remaining rejection, and the arguments presented would be applicable. As such, the prior arguments still apply with respect to the rejection under 35 U.S.C. § 103(a).

Pfitzmann and Kaminsky are not prior art

The Examiner makes several other assertions in responding the Applicant's arguments that appear unsupported. The Examiner states that "Microsoft Passport is the first well known federated identity management protocol" (*see* Office Action dated February 26, 2007, page 3), and cites to Federated Identity-management Protocols by Birgit Pfitzmann and Michael Waidner, published in 11th International Workshop on Security Protocols, pages 153-174 (2003) ("Pfitzmann"). This reference (and User Authentication and Remote Execution Across Administrative Domains by Michael Kaminsky, Ph.D. Thesis, Massachusetts Institute of Technology (September 2004) ("Kaminsky")) is published after the filing date of the patent application, and so is not available as a reference under 35 U.S.C. §§ 102 or 103. Responding to an argument that traverses a rejection is nothing more than a buttressing of the original rejection. Therefore, the response to an argument needs to be supported by the prior art: a reference that does not qualify as prior art should not be used in responding to an argument.

Microsoft Passport does not teach the claimed invention

Even if we assume the Examiner's assertion that "Microsoft Passport is the first well known federated identity management protocol" is correct (whether or not supported by proper prior art), this assertion is irrelevant. The claims are not directed to a federated identity management protocol: the claims are directed toward a method and apparatus for cross domain authentication. Some of the claims do mention federation access policy (*see, e.g.*, claims 1 and 38). But federated identity as purportedly used in Microsoft Passport is a very different concept from a federation access policy as claimed. According to Pfitzmann, federated identity management is designed to address "[t]he high-level goal of enterprises . . . to simplify user management in an increasingly dynamic world. In particular, they [enterprises] want to benefit from user registration done in other places for their own user management" (*see* Pfitzmann, section 1 on page 1).

In contrast, the federation access policy of the claims "specifies rights for any identity in the federated identity space" (*see* specification, page 3, lines 16-17). "[T]he administrator of the local identity space decides who in the federation can access the information served by the local identity space" using the federation access policy (*see* specification, page 4, lines 13-14). "Federation access policy 125, as described above, is used to specify which external users, once authenticated, are authorized to access which local resources" (*see* specification, page 5, lines 12-13). Thus, the only thing in common between the federation access policy of the claimed invention and the federated identity management of Microsoft Passport is a form of the word "federation". Microsoft Passport, by itself, does not anticipate or make obvious even one feature of the claims, let alone any one claim as a whole.

Further, the Examiner is grossly overstating Pfitzmann. Pfitzmann states "Figure 1 gives an overview of browser-based federated identity-management protocols. The first such protocol was Microsoft Passport. It is not published . . ." (*see* Pfitzmann, section 2 on page 3). There are two very significant points in this quote. First, Pfitzmann did not assert that Microsoft Passport was the first federated identity-management protocol: Pfitzmann asserted that Microsoft Passport was the first browser-based federated identity management protocol. To say that Microsoft Passport was "the first well known federated identity management protocol" is an incorrect interpretation of Pfitzmann. In fact, the Examiner's own references belie the truth of the Examiner's statement: according to Kormann, "Kerberos [1] is an example of a system where users provide a password and receive a ticket in exchange. The ticket can be used to authenticate users to different network services" (*see* Kormann, section 1 on page 1). According to Kormann, Kerberos was available at least as far back as 1988 (*see* Kormann, reference [1]). This shows that Microsoft Passport was not the "first well known federated identity management protocol", as the Examiner asserts.

Microsoft Passport Protocol was unpublished at the time of filing – its operation was secret

The second significant point from this quote is that the Microsoft Passport protocol was "not published". As the Applicant has argued before, Microsoft Corporation is known to hide details, for numerous reasons. If the Microsoft Passport protocol was still unpublished in 2003, it was certainly unpublished in 2001, when the Applicant filed the patent application. As such,

the implementation of Microsoft Passport was not publicly known, which defeats the Examiner's argument that the features of the claimed invention were publicly known. At best, Microsoft Passport was one of the first browser-based federated identity management protocols used by significant numbers of people. Any other statement reads too much into Pfitzmann.

A related problem with the Examiner's reliance on the Microsoft Passport protocol is that a person skilled in the art was not enabled to implement the protocol in 2001. As noted above, Pfitzmann explicitly stated that the Microsoft Passport protocol was "not published". If the protocol was "not published", then a person skilled in the art would not be enabled to make and use the protocol. But a reference must enable a person skilled in the art to make and use the invention if the reference is to support a proper rejection of a claim in a patent application (*see* M.P.E.P. § 2121 *et seq.*). If a reference does not enable the claimed invention, then the claims cannot be rejected over the reference. Given that the Microsoft Passport protocol was unpublished, it cannot be enabled, and therefore cannot support a rejection of the claims under 35 U.S.C. §§ 102-103.

The Examiner next states that "[t]he view of Pfitzmann is confirmed by Kaminsky . . ., which makes references throughout the paper to Microsoft" (*see* Office Action dated February 26, 2007, page 3). The Examiner goes on to say that "Applicant's arguments regarding the inapplicability of Windows 2000 seem less persuasive when considered in the light of the opinions of the leading scholars (Pfitzmann, Waidner, Kaminsky) on this subject. These scholars assert Passport from Microsoft as the first well known protocol in the field. Because they also discuss Windows as a successor to Passport, Applicant's arguments regarding the inapplicability of Windows 2000 seem less persuasive" (*see* Office Action dated February 26, 2007, page 3).

There are three problems with the Examiner's logic. First, Pfitzmann does not mention Microsoft Windows 2000 anywhere. Given that Pfitzmann is describing federated identity management protocols in general and was published well after the release of Microsoft Windows 2000, Pfitzmann's failure to mention Microsoft Windows 2000 strongly suggests that Microsoft Windows 2000 does not include such a protocol.

Kaminsky does not support the Examiner's position

The Examiner's statement that Kaminsky supports Pfitzmann is even more puzzling. The Examiner argues that because Kaminsky "makes reference throughout the paper to Microsoft" (*see* Office Action dated February 26, 2007, page 3), this fact somehow confirms the view of Pfitzmann. The Applicant asserts that Kaminsky makes minimal and irrelevant references to Microsoft: Kaminsky uses the name "Microsoft" a grand total of six times, including once in the table of contents and twice in the bibliography. That leaves three occurrences of "Microsoft" in the body of Kaminsky. Kaminsky refers to Microsoft Windows 2000 on page 16 of his thesis, and twice on page 64 of his thesis. But on page 16, Kaminsky is discussing the problem with network file systems, not federated identity management. And on page 64 Kaminsky discusses domains in Microsoft Windows 2000.

Despite Kaminsky's six references to "Microsoft", nowhere does Kaminsky mention Microsoft Passport. Without even a mention of Microsoft Passport, and with emphasis on aspects of Microsoft Windows 2000 that are not part of Microsoft Passport, it seems a great leap of logic for the Examiner to conclude that Kaminsky confirms Pfitzmann's view.

Pfitzmann and Kaminsky do not describe Microsoft Windows 2000 as a successor to Microsoft Passport

The second problem with the Examiner's logic is that there is no other evidence to suggest that Microsoft Windows 2000 was ever intended as a successor product to Microsoft Passport. The mere fact that both Microsoft Passport and Microsoft Windows 2000 are products of Microsoft Corporation does not imply that either is a successor to the other. In fact, given that both Pfitzmann and Kaminsky were written after both Microsoft Passport and Microsoft Windows 2000 had been released, the fact that neither reference discusses both products strongly suggests that neither product is a successor to the other. Certainly, neither author describes Microsoft Windows 2000 as a "successor" to Microsoft Passport, but both authors clearly had the opportunity to make such a statement. The Examiner's conclusion that Pfitzmann and Kaminsky "discuss Windows as a successor to Passport" is thus totally unsupported by either reference or any other evidence of record. Thus, the Examiner's assertion that Microsoft Windows 2000 includes the functionality offered by Microsoft Passport is entirely unsupported, and the Pfitzmann and Kaminsky references both suggest the Examiner's conclusion is wrong.

To illustrate how the Examiner's logic is incorrect, consider, for example, Microsoft Flight Simulator 1.00, which was released around 1982 and so existed long before, say, Microsoft Windows 2000 or Microsoft Windows XP were released. Under the Examiner's logic, that would mean that Microsoft Windows 2000 or Microsoft Windows XP is a successor to Microsoft Flight Simulator 1.00. But neither Microsoft Windows 2000 nor Microsoft Windows XP offers the functionality of Microsoft Flight Simulator 1.00, and so neither product is a "successor" to Microsoft Flight Simulator 1.00, except in the irrelevant chronological sense.

In fact, there is other strong evidence to suggest the two products are unrelated. Microsoft continues to promote technology that is the current successor to Microsoft Passport: this technology is currently called Windows Live ID (*see, e.g.*, Windows Live ID, https://accountservices.passport.net/ppnetworkhome.srf, a copy of which is attached hereto). Windows Live ID describes itself as being designed to "[c]reate your sign in credentials (e-mail and password) once, then use them everywhere on the Windows Live ID service. You can even set the site to remember your credentials for you!" (*see* Windows Live ID, https://accountservices.passport.net/ppnetworkhome.srf). Windows Live ID even states that "Windows Live ID works with Passport Network sites" (*see* Windows Live ID, https://accountservices.passport.net/ppnetworkhome.srf). This is exactly the functionality Microsoft Passport offered previously (*see, e.g.*, Kormann).

Further suggesting that Microsoft Windows 2000 was not intended to be a successor to Microsoft Passport is their different usage. Microsoft Windows 2000 is an operating system; Microsoft Passport is a web application. An operating system cannot, by itself, replace a web application, or vice versa.

The third problem with the Examiner's logic is that the Examiner is wrong to describe "Passport from Microsoft as the first well known protocol in the field" (*see* Office Action dated February 26, 2007, page 3). As noted above, Pfitzmann states that, as of 2003, the protocol used by Microsoft Passport was "not published", and Kaminsky does not even mention Microsoft Passport. If the protocol was unpublished, it can hardly be called "well known". The protocol used by Microsoft Passport might have been the widely *used*, but there is an enormous difference between being the protocol being used and the protocol being known or understood.

In addition, as noted above, Pfitzmann did not assert that Microsoft Protocol was the first federated identity management protocol: Pfitzmann asserted that Microsoft Passport was the first

browser-based federated identity management protocol. Thus, the Examiner is reading Pfitzmann far more broadly than Pfitzmann ever intended.

REJECTIONS UNDER 35 U.S.C. § 102(a)

Claim 1 is directed toward a cross-domain authentication apparatus, the apparatus comprising: a first computer on a first domain and a second computer on a second domain; a network connecting the first and second computers; a secret shared between the first and second computers; and a federation access policy identifying access permission on the first computer on the first domain for a user local to the second computer on the second domain over the network.

In contrast, Kormann describes the operation of Microsoft Passport. Microsoft Passport is a system designed to implement "single signon", which allows a user to remember only one username and password and be authenticated for multiple services. Initially, the Microsoft Passport server and the merchant web page agree on an encryption key to be used in encrypting communications between the Microsoft Passport server and the merchant. When a user requests a web page from a merchant that requires authentication, the merchant web page redirects the request to the Microsoft Passport server. The Microsoft Passport server requests the user's credentials (e.g., username and password). After the user is authenticated to the Microsoft Passport server, the Microsoft Passport server redirects the user back to the merchant web page providing authentication information that is encrypted using the agreed-upon key. This model permits "single signon" in that if the user later visits another merchant web page that also requires authentication, when the request is redirected to the Microsoft Passport server, the Microsoft Passport server can provide the encrypted authentication information immediately without the user having to provide the authentication information again.

The differences between Microsoft Passport, as described by Kormann, and the claimed invention are numerous. The first point of distinction is that the claimed invention involves only two domains, with the user local to one of the domains. In Microsoft Passport, there are actually three domains involved: the domain to which the user belongs, the domain of the merchant, and the Microsoft Passport server (which resides in its own domain). In particular, the user is not local to the domain including the Microsoft Passport server.

That the user is not local to the Microsoft Passport domain is apparent from several well known points. First, Microsoft Passport permits any users to achieve "single signon": there is no

limitation based on the domain of the user. For example, Microsoft Passport is not described as available to only people whose domains are "passport.com". This point is also emphasized by the fact that the login ID for Microsoft Passport is the user's e-mail address, rather than just a user ID (i.e., the login ID is "username@domain.com", rather than just "username"). Second, to protect the integrity of the personal information stored on the Microsoft Passport server, it would be a major security risk for users to have local accounts on the Microsoft Passport domain. Such an account would permit the user direct access to the network, rather than the controlled access through proxy requests (if all requests must be made through a proxy, direct requests can be recognized as attacks and ignored or otherwise handled).

It is important to remember what a "domain" is. According to the specification, a "domain" is an "identity space" (*see, e.g.*, specification, page 2, line 26). This is entirely consistent with "domains" as normally understood in the art: a domain is a group of computers administered as a unit; domains are defined by Internet Protocol (IP) addresses (*see, e.g.*, define:domain, http://www.google.com/search?hl=en&q=define%3Adomain&btnG=Google+Search, a copy of which is attached hereto). For example, in Figure 1 of Kormann, the computer with the browser (and which the user is currently using) could be part of a local network operated by a business and administered in common, and would be in one domain. But the Microsoft Passport server, which is not operated by the business and is not administered by the same person who administers the local network, is not in that domain: that server is in an entirely different domain. And the merchant web page (in Figure 1 of Kormann, the web page is one of IBM.com) is in yet a third domain.

Thus, it should be clear that in Kormann, there are three domains involved. And this makes sense: Microsoft Passport is concerned with providing single signon functionality: "a system whereby users need only remember one username and password, and [authentication] can be provided for multiple services" (*see* Kormann, section 1 on page 1). In other words, Microsoft Passport, as described by Kormann, is concerned with providing a way for a merchant to be assured that a user is who he says he is independent of the computer and domain from which the user is requesting access to the merchant's services. A third party, trusted by all merchants to perform authentication of user identity, enables the single signon functionality.

But claim 1 is not directed toward single signon functionality. Instead, claim 1 provides a framework in which the "federation access policy identify[ies] access permission on the first computer on the first domain for a user local to the second computer on the second domain over the network" as recited in claim 1, can be implemented. A detailed example is provided in the specification on pages 5-10: the following provides a brief summary. A user in the BluePark domain requests access to a resource from the GreenPark domain. Before granting access to the GreenPark resource, the GreenPark system requests that the user be authenticated in the BluePark domain. Once the user authenticated in the BluePark domain, this information is communicated to the GreenPark domain. The GreenPark domain then determines the access rights the user has to the requested resource, and provides the appropriate level of access.

Thus, using Microsoft Passport would leave a large hole in the operation of the claimed invention: Microsoft Passport does not provide any information about the domain from which the user is requesting the resource. In other words, Microsoft Passport would authenticate the user *to the Microsoft Passport domain*, not the domain to which the user is local. Without this information, the first domain cannot know to which domain the user is local, and cannot apply the appropriate access control.

Consider, for example, a situation where there are three domains: domain 1 contains a resource, and domains 2 and 3 each have access to the resource, but at different levels (for example, users on domain 2 can read and write to the resource, but users on domain 3 can only read the resource). Further assume that there is one user Jack who is common to both domains. Using Microsoft Passport, domain 1 would only be certain of Jack's identity; domain 1 would not know whether Jack is local to domain 2 or to domain 3 (or perhaps to an entirely different domain which is not granted any access to the resource). As a result, in contrast to the claimed invention, domain 1 cannot determine the appropriate level of access to grant to Jack.

This is one reason why Microsoft Passport does not teach or suggest the claimed invention: the user is authenticated by the domain to which the user is local. This point is reinforced in new dependent claim 48, where the second domain includes means for authenticating the user. Claim 48 makes it clear that the authentication is handled within the second domain (and not relying a third-party authentication system, such as Microsoft Passport).

It is also worth noting that anyone can create a Microsoft Passport account. Thus, anyone can be authenticated to Microsoft Passport. But domains, such as the first domain and second

domain of claim 1, can be more restrictive: generally, only users explicitly permitted to use those systems will have accounts on those systems. If a hacker were able to spoof data as coming from the second domain in claim 1 and Microsoft Passport were being used to authenticate the hacker, then the first domain could potentially be fooled into providing access to secure resources to a hacker who should not be granted access. But with authentication performed locally on the second domain, the hacker would be unable to spoof the authentication of the second domain. (It is also true that the shared secret would be unknown to the hacker, and so would help prevent the resource being accessed improperly, but that fact does not address the problem that Microsoft Passport would indicate the hacker is authenticated even though he is not local to the second domain.)

A second difference between the claimed invention and Kormann relates to this first difference. Claim 1 recites that there is "a secret shared between the first and second computers". This means that the secret is shared between machines in the first and second domains. As argued above, the Microsoft Passport server described by Kormann is in a third domain. Thus, while Kormann describes communications between the Microsoft Passport server and the merchant encrypted with a previously established key, the key in question is not shared between the domain with the resource and the domain with the user, as claimed.

A third difference between the claimed invention and Kormann is that claim 1 recites "a federation access policy identifying access permission on the first computer on the first domain for a user local to the second computer on the second domain over the network". As described in the specification and recited clearly in the claims, the federation access policy relates to access permission. In contrast, while the Examiner describes Microsoft Passport as "the first well known federated identity management protocol" (which is a misstatement on several levels: see arguments above regarding the Examiner's response to the Applicant's arguments), identity management is a totally separate issue from a federation access policy. Microsoft Passport does not define access permissions.

Because Kormann does not teach or suggest cross-domain authentication using only two domains, a secret shared between the two domains, or a federation access policy, claims 1 and 48 are patentable under 35 U.S.C. § 102(a) over Kormann. Accordingly, claims 1 and 48 are allowable, as are dependent claims 2-18 and 47.

In rejecting claims 2-3, 25-26, and 34-35, the Examiner makes a sweeping rejection based on Kormann's passing mention of the use of HTTP redirection in the use of Microsoft Passport. The Examiner thus suggests that this one mention of HTTP redirection anticipates any possible use of HTTP proxies.

First of all, the Applicant respectfully points out that HTTP redirection and HTTP proxies are not the same thing. HTTP redirection merely involves changing the destination web page of a request. As clearly shown in Figure 1 of Kormann, the HTTP redirection is requested by the merchant and the Microsoft Passport server directly: there is no mention or suggestion of a proxy, nor is there a need for a proxy in Kormann. In contrast, the proxies of the claims are additional machines that are part of the system between the computers. For example, the Examiner is referred to FIG. 1 of the patent application, where each domain is shown as including an HTTP Proxy Server. This description is further bolstered by page 2, lines 23-25 of the specification, which describe the use of proxy servers. The fact that the proxies recited in the claims can redirect communication as appropriate does not mean that an example of HTTP redirection teaches a proxy server.

Second, the various claims recite more specific elements that a general HTTP redirection, as taught by Kormann, does not include. For example, claim 2 recites "the proxy designed to request an authentication challenge of the user from the second computer"; claim 3 recites "an HTTP forward proxy coupled to the second computer designed to respond to the authentication challenge for the user and forward the authentication to the reverse proxy"; claim 25 recites "sending a challenge authentication from a reverse proxy at the first computer to a forward proxy at the second computer"; claim 26 recites "sending a challenge authentication from a reverse proxy includes redirecting the user to a mediator coupled to a forward proxy at the second computer"; claim 34 recites "integrity-protecting the response using the session secret key at a reverse proxy of the first computer before sending the response to a forward proxy of the second computer over the network"; and claim 35 recites "integrity-verifying the response at a forward proxy of the second computer before sending the response to the user at the second computer". None of these elements are taught or suggested by HTTP redirection.

Because Kormann does not teach or suggest any additional elements during an HTTP redirection, claims 2-3, 25-26, and 34-35 are patentable under 35 U.S.C. § 102(a) over Kormann. Accordingly, claims 2-3, 25-26, and 34-35 are allowable, as are dependent claims 4 and 27-28.

In rejecting claims 5-8, 10-12, 14-17, 20, 24, 27, 33, and 37-44, the Examiner makes a sweeping rejection based on Kormann's discussion about authentication. The Examiner apparently is suggesting that authentication is the same thing as access policy implementation and any number of other elements of the claims.

The Applicant respectfully suggests that these claims include numerous features not taught by Kormann. For example, claim 5 recites "a security module designed to implement the federation access policy"; claim 6 recites "the federation access policy includes an access for a role identity; and the apparatus further comprises an identity mapping from the user to the role identity"; claim 7 recites "the identity mapping is designed to enable access to a resource on the first computer across different formats and encodings of user names"; claim 8 recites "an access control entry in the federation access policy designed to enable access to a resource on the first computer by a user on the second computer"; claim 10 recites "a permission for the user on the second computer that is equal to or less than a permission available to the second user on the first computer"; claim 11 "a public key certificate for the user on the second computer whose access is controlled by the access control entry"; claim 12 recites "means for automatically retrieving from the second computer the public key certificate for the user on the second computer without human intervention"; claim 14 recites "the federation access policy is designed to permit a second user on the first computer to remove or modify the access control entry, the second user having a privilege to remove or modify the access control entry"; claim 15 recites "the second user is the user who defined the access control entry"; claim 16 recites "the access control entry is designed to enable access to the resource on the first computer across different formats and encodings of user names"; claim 17 recites "the federation access policy includes a resource to which the user is permitted access"; claim 20 recites "authenticating the user at the second computer"; claim 24 recites "challenging the user includes sending a challenge authentication from the first computer to the second computer"; claim 27 recites "authenticating the user using the mediator"; claim 33 recites "integrity-protecting a response using the session secret key"; claim 37 recites "determining whether the user has permission to access the resource"; claim 38 recites "checking a federation access policy to determine whether the user has permission to access the resource"; claim 39 recites "using an identity mapping in the federation access policy to map the user to a local identity; and checking that the local identity is permitted to access the

resource"; claim 40 recites "using the identity mapping in the federation access policy to map the user to the local identity, allowing for different formats and encodings of user names between the first and second computers"; claim 41 recites "using an access control entry in the federation access policy to determine if the user is permitted to access the resource"; claim 42 recites "using the access control entry in the federation access policy to determine if the user is permitted to access the resource, allowing for different formats and encodings between the first and second computers"; claim 43 recites "authenticating the user using a third party as a mediator"; and claim 44 recites "maintaining channel integrity between the first computer and the second computer over the network". None of these elements are taught or suggested by authentication.

Because Kormann does not teach or suggest any of the features recited in claims 5-8, 10-12, 14-17, 20, 24, 27, 33, and 37-44, claims 5-8, 10-12, 14-17, 20, 24, 27, 33, and 37-44 are patentable under 35 U.S.C. § 102(a) over Kormann. Accordingly, claims 5-8, 10-12, 14-17, 20, 24, 27, 33, and 37-44 are allowable, as are dependent claims 9, 13, 21, 25-26, 28, and 34-35.

Claim 9 is directed toward an apparatus according to claim 8, wherein the federation access policy is designed to permit a second user on the first computer to define the access control entry without requiring assistance from an administrator.

In rejecting claim 9, the Examiner cites paragraphs of section 1 of Kormann as teaching "permitting a second user to have access without requiring assistance from an administrator" (*see* Office Action dated February 26, 2007, page 6). The Applicant respectfully points out that the Examiner has not read claim 9 in its entirety. Claim 9 is not directed toward a user having access without assistance: claim 9 is directed toward "a second user on the first computer to define the access control entry without requiring assistance from an administrator". Nowhere does Kormann say anything about an access control entry, let alone who gets to define the access control entry. The Examiner is not supposed to ignore words in the claims in issuing a rejection (*see, e.g.*, M.P.E.P. §§ 2143.03 and 2173.06: "All words in a claim must be considered in judging the patentability of a claim against the prior art" (citing *In re Wilson*, 424 F.2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)).

The Examiner goes on to argue that "in Windows 2000, . . . a second user (e.g., another administrator) may have access without requiring assistance from the other administrator" (*see* Office Action dated February 26, 2007, page 6). There are two problems with this assertion.

First, by the Examiner's own admission, "Passport differs from Windows 2000" (*see* Office Action dated February 26, 2007, page 6). But Kormann describes Microsoft Passport, not Microsoft Windows 2000. Thus it is irrelevant to the analysis of Kormann what happens in Microsoft Windows 2000: what matters is how Microsoft Passport operates. And the Examiner even admits that "Passport does not promote the administrator to block users in such fashion; Passport differs from some versions of Windows in how Kerberos is used" (*see* Office Action dated February 26, 2007, page 6). This simultaneously shows that what Microsoft Windows 2000 does is irrelevant to Microsoft Passport (and so is irrelevant to whether the claims are patentable under 35 U.S.C. § 102(a) over Kormann) and that the Examiner was wrong to earlier postulate that Microsoft Windows 2000 was a successor to Microsoft Passport.

Second, even if "Passport permits a second user to have access without requiring assistance from an administrator" (*see* Office Action dated February 26, 2007, page 6), such a user would still be using Microsoft Passport to be authenticated. And this still fails to show that Microsoft Passport has anything to do with defining an access control entry (which Microsoft Passport does not use).

Because Kormann does not teach or suggest a user on the first computer to define the access control entry without requiring assistance from an administrator, claim 9 is patentable under 35 U.S.C. § 102(a) over Kormann. Accordingly, claim 9 is allowable, as is dependent claim 10.

Claim 19 is directed toward a method for performing cross domain authentication, the method comprising: receiving a request for a resource on a first computer on a first domain from a user local to a second computer on a second domain over a network; challenging the user to be authenticated; authenticating the user in the second domain; informing the first computer on the first domain that the user is authenticated in the second domain; and accessing the resource from the first computer on the first domain using the second computer on the second domain.

As argued above with reference to claim 1, the Microsoft Passport server used to perform authentication in Kormann is in a third domain separate from the user domain and the merchant domain. In contrast, claim 19 recites "authenticating the user in the second domain", where the user is local to the second computer on the second domain. In other words, the authentication is not done in a third-party domain, which is what Kormann teaches.

Because Kormann does not teach or suggest authenticating the user in the second domain, claim 19 is patentable under 35 U.S.C. § 102(a) over Kormann. Accordingly, claim 19 is allowable, as are dependent claims 20-46.

REJECTIONS UNDER 35 U.S.C. § 103(a)

With respect to claims 1-46, as these claims are rejected under 35 U.S.C. § 103(a) as being unpatentable over "Comptech Article" for the reasons presented in the previous Office Actions, the Applicant incorporates herein all previous arguments made regarding the patentability of claims 1-46 over "Comptech Article".

Claim 47 is directed toward a cross-domain authentication apparatus according to claim 1, wherein the first domain is different from the second domain.

In rejecting claim 47, the Examiner argues that "Comptech Article" "teaches the use of multiple domains in which the domains are different" (*see* Office Action dated February 26, 2007, page 7). But nowhere does "Comptech Article" mention "multiple domains". "Comptech Article" does describe different logon processes, depending on whether the logon in local or domain. But neither logon process mentions "multiple domains". And the fact that there are two different logon processes that can be used does not support the assertion that multiple domains are used.

Because "Comptech Article" does not teach or suggest the use of multiple domains, claim 47 is patentable under 35 U.S.C. § 103(a) over "Comptech Article". Accordingly, claim 47 is allowable.

REMARKS IN THE OFFICE ACTION DATED JANUARY 10, 2007

In the Office Action dated January 10, 2007, the Examiner asserted several facts. In the response to the Office Action dated January 10, 2007, the Applicant responded to these assertions. Because the Examiner marked that Amendment After Final as "Do Not Enter", the Applicant resubmits these arguments, so that they are of record in this patent application.

In the Office Action dated January 10, 2007, the Examiner asserts that several facts "seem to be accepted by Applicant". The Examiner's assertion is unsupported, and in fact contradicted, by the record.

The Applicant has never accepted that Microsoft Windows 2000 had federation policy regarding user authentication across domains in the year 2000

The Examiner states that the Applicant has accepted that "[a]lready in the year 2000, before the filing date of this application, Windows 2000 as reported to the media (as evidenced by the cited references in the prosecution history of this application) had federation policy regarding user authentication across domains" (*see* Office Action dated January 10, 2007, page 2; emphasis in original). The Applicant respectfully disagrees.

First, the "cited references" to which the Examiner refers were all published after the filing date of the patent application. As such, none of the "cited references" can properly be considered to describe Microsoft Windows 2000 as it existed "in the year 2000". Further, the "cited references" are not proper prior art, and so should not be considered by the Examiner in rejecting the pending claims.

Second, the Applicant recognizes that, at some point, Microsoft Windows 2000 included some features similar to those described in "Comptech Article". But the Applicant has never indicated when those features were added to Microsoft Windows 2000, and has certainly never acknowledged that those features were part of Microsoft Windows 2000 before the filing date of this patent application, let alone as of the original release date of Microsoft Windows 2000. This supposedly "accepted fact" of the Applicant has been one of the points of contention between the Applicant and the Examiner: exactly when did Microsoft Windows 2000 include the features the Examiner asserts render the claimed invention obvious? The Applicant asserts that the Examiner bears the burden of proof regarding when these features became a part of Microsoft Windows 2000: the Examiner is not entitled to simply assume that these features have been part of Microsoft Windows 2000 since its original release date.

The Applicant respectfully reminds the Examiner that the Examiner bears the burden of establishing a prima facie case for an obviousness rejection. According to M.P.E.P. § 2142, "The legal concept of prima facie obviousness is a procedural tool of examination which applies broadly to all arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process. . . . The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness" (citations omitted).

Since one (but not the only) point of contention between the Examiner and the Applicant is when the features in question were included in Microsoft Windows 2000 and the Examiner "bears the initial burden of factually supporting any establishing a prima facie conclusion of obviousness", it is up the Examiner to show that these features were part of Microsoft Windows 2000 before the filing date of this application. The Examiner has repeatedly pointed to "Comptech Article" as teaching the features in question. But even the Examiner admits that "Comptech Article" was not published before the filing date (*see, e.g.*, Interview Summary submitted on September 20, 2005). According to the Examiner, "the Office cited ["Comptech Article"] as a teaching regarding Windows 2000 rather than being prior art being published in the year 2000" (*see* Office Action dated June 9, 2006, page 2). If the reference is being cited not because it was "published in the year 2000" (which "Comptech Article" was not), then it would seem evident that the Examiner agrees that "Comptech Article" was not published before the filing date of the application. Further, the Examiner has never suggested that "Comptech Article" was published before its stated date of October 28, 2001.

Since "Comptech Article" does not provide the factual support required by M.P.E.P. § 2142, then the Examiner would need to provide that factual support from some other source. The Examiner has failed to provide this factual support from any other source, instead insisting that "Comptech Article" must describe the original release of Microsoft Windows 2000. Indeed, the Examiner stated that "[t]he Office cannot find Applicant to be persuasive [as to which release of Microsoft Windows 2000 the author of "Comptech Article" referred] because the author did not mention that his discussion was meant to be for only some releases; one would surely expect an author to have noted more than one release if the author was aware of the critical differences between the release" (*see* Office Action dated June 9, 2006, page 2). The Applicant points out that the Examiner's reasoning depends on two assumptions, neither of which has been shown to be reasonable, let alone correct. First, the Examiner has assumed that the author of "Comptech Article" was aware of these "critical differences". But if the author of "Comptech Article" was not aware that these "critical differences" exist, then the author might not have drawn these differences to the reader's attention. The Examiner has not shown that the author of "Comptech Article" was aware of these "critical differences". As such a showing would be needed to provide the factual support for a rejection under 35 U.S.C. § 103(a) as explained in M.P.E.P. § 2142, the assumption must be proven: it cannot be summarily drawn.

Second, the Examiner assumes that the author of "Comptech Article" intended the article to cover all versions of Microsoft Windows 2000. This conclusion can be seen from the fact that the Examiner maintains the author would have noted the "critical differences" between versions of Windows 2000, assuming the author of "Comptech Article" was aware of the "critical differences". But this assumption is also unwarranted. The conclusion could just as easily be reached the other way: the author made no mention of other versions of Microsoft Windows 2000 because he assumed everyone had updated their software to the latest version. Microsoft Corporation routinely encourages users to run only the very latest versions of their software: Microsoft Corporation even refuses to support versions of software that are sufficiently out-of-date. Their operating systems, such as Microsoft Windows XP, actively check for updates and download and install those updates automatically.

Even more to the point, a user cannot download current updates to Microsoft Windows XP until they have installed Service Pack 2 (*see, e.g.*, Microsoft Windows Update, http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us, a copy of which is attached hereto). Thus, it is entirely reasonable that the author of "Comptech Article" could assume everyone was updated to the latest version of Microsoft Windows 2000, and did not need to address "critical differences" between versions of Microsoft Windows 2000.

These assumptions by the Examiner are an effort to shift the burden to the Applicant. Essentially, the Examiner has required the Applicant to show why "Comptech Article" does not make obvious the claimed invention, even though the Examiner has not established a prima facie case of obviousness. More specifically, the Examiner has required the Applicant to show why the features in question were not part of the original release of Windows 2000. This shifting of the burden is inappropriate: it is the Examiner's burden to show that the features in question were in fact part of Windows 2000 before the filing date of the patent application. The Examiner has failed to meet this burden.

Thus, the Examiner's assumptions about the author of "Comptech Article" are unwarranted. Given that the Examiner has acknowledged that "Comptech Article" was not published before the filing date of the patent application, the Examiner has failed to provide factual support for the rejection under 35 U.S.C. § 103(a), as required by M.P.E.P. § 2142. Thus, the Examiner has failed to establish a prima facie case of obviousness.

The Applicant has never accepted that the claims would not be patentable if Windows 2000 had federation policy regarding user authentication across domains

The Examiner next states that the Applicant has "accepted" that "[c]laims of this application would not be patentable if Windows 2000 in the year 2000 (as evidenced by the cited references in the prosecution history of this application) had federation policy regarding user authentication across domains" (*see* Office Action dated January 10, 2007, page 2; emphasis in original). The Applicant disagrees. Although the Applicant has argued at length that "Comptech Article" is not available as a reference in this patent application, the Applicant has never acknowledged that the claims would not be patentable over Microsoft Windows 2000 if, in the year 2000, Microsoft Windows 2000 included the features described in "Comptech Article". To the contrary, the Applicant has argued why the claims are not obvious over "Comptech Article" in the response to every Office Action, even assuming arguendo that "Comptech Article" were proper prior art (which the Applicant asserts it is not). The Applicant does not intend to present again the arguments in support of this point, but instead refers the Examiner to pages 11-13 of the response to the Office Action dated September 8, 2004; pages 9-10 of the response to the Office Action dated April 21, 2005; pages 10-17 of the response to the Office Action dated June 9, 2006; and pages 19-29 of the response to the Office Action dated September 21, 2006.

The Applicant notes that the Examiner has not responded to any of these arguments, except in making the comment that "Applicant argued that the reference does not teach a 'shared secret.' A shared secret is a secret that is shared. A password can be a secret. How can a password not be a secret?" (*see* Office Action dated April 21, 2005, page 2). The Applicant responded to this comment in the response to the Office Action dated April 21, 2005. To this day, the Examiner has not addressed the deficiencies of the reference, even assuming that "Comptech Article" were proper prior art. In particular, the Examiner has never responded to the Applicant's arguments as to why the claimed invention is patentable over "Comptech Article": please refer to the arguments in the previous responses cited above.

The Examiner appears to be drawing an improper inference from the Applicant's refusal to submit an affidavit

It appears that the Examiner is concluding that, because the Applicant has not filed an affidavit that Microsoft Windows 2000 did not include the features described in "Comptech

Article" as of its original release, that this is equivalent to the Applicant acknowledging that Microsoft Windows 2000 did, in fact, include those features in its original release. The Applicant respectfully disagrees. The refusal to submit the requested affidavit is not because the Applicant believes the features in question were part of Microsoft Windows 2000 in the year 2000; the refusal is based solely on the fact that the Applicant cannot attest, under penalty of perjury, that the features in question were not part of Microsoft Windows 2000 in the year 2000. But the fact that the Applicant cannot attest to truth of particular facts does not automatically mean that those facts are necessarily false. For example, the facts that the Examiner wanted the Applicant to attest to might be secret facts. The Applicant's refusal or inability to attest to such facts does not mean the facts are necessarily false.

There is an enormous semantic difference between refusing to say "X is true" and saying "X is false". A refusal to say "X is true" simply means that the party cannot state as a certainty that "X" is true; "X" could still be true anyway. For example, if one were to ask most people the question "Is 5,992,830,235,524,142,758,386,850,633,773,258,681,119 a prime number?", most people would have no clue whether the answer is "yes" or "no": they would not know whether that particular number (admittedly, a large number) is prime or not. But the fact the people cannot answer "yes" to this question does not automatically mean that this number is not prime. In fact, 5,992,830,235,524,142,758,386,850,633,773,258,681,119 is a prime number (*see* Primes with 10 to 100 digits, http://primes.utm.edu/lists/small/small.html, a copy of which is attached hereto). Yet this is exactly the improper type of logic the Examiner appears to be applying in this case. This is inappropriate: the fact that the Applicant is unable to supply the requested affidavit is not equivalent to an acknowledgement that Microsoft Windows 2000 included the features in question in its original release.

In addition, as argued above and previously, the Applicant has no burden to prove that Microsoft Windows 2000 did not include the features described in "Comptech Article" as of its original release date. To the contrary, the burden is on the Examiner to establish that Microsoft Windows 2000 included those features as of its original release date. The Examiner bears the burden of establishing a prima facie case for obviousness; one necessary element of a prima facie case for obviousness is that the facts being used to reject the claims were known before the filing date of the patent application. The Applicant's refusal to submit the requested affidavit does not satisfy the Examiner's burden of establishing a prima facie case for obviousness. The Examiner

has failed to meet this burden, instead attempting to shift the burden to the Applicant to disprove the Examiner's assumption. As stated repeatedly, this burden-shifting is inappropriate.

The Examiner emphasizes "as reported to the media" as support for the rejection

At least twice in the Office Action dated January 10, 2007, the Examiner stated that "Comptech Article" shows how Microsoft Windows 2000 was "reported to the media" (*see* Office Action dated January 10, 2007, pages 2-3). The Applicant would like to point out that the "reports to the media" to which the Examiner refers are the references that the Applicant maintains are not proper prior art. The Examiner is within his right to change the grounds of rejection to a new reference, if the Examiner can find such a reference, although such a new rejection would require a new, non-final Office Action. But even then, the Examiner would still need to show that the reference was published before the filing date of the application or establishes conclusively what was "publicly known" before the filing date of the application, and documents published after the filing date of the application do not meet that requirement. Again, one of the central points of contention between the Applicant and the Examiner is when the information in question was known. That some information was "reported to the media" at some point in time does not establish that such information was publicly known before the filing date of the application.

To the extent the "reports in the media" might be considered to support a claim rejection, the "reports in the media" can only be considered descriptive as to what was made public about Microsoft Windows 2000 at the time the "reports" were made. Thus, for example, "Comptech Article" can only be considered a description of what was made public about Microsoft Windows 2000 at the time "Comptech Article" was published: October 2001, well after the filing date of this patent application. To assert that "Comptech Article" describes what was publicly known about Microsoft Windows 2000 at any earlier time is to read more into the "report in the media" than it deserves. The Examiner has failed to establish what features Microsoft Windows 2000 included as of the year 2000. The media reports upon which the Examiner relies, as they were published after the filing date of the patent application, do not establish what features Microsoft Windows 2000 was reported to the media as including in the year 2000.

Microsoft Windows 2000, without a description of what it included before the filing date of the patent application, is not prior art

The Examiner states that "Applicant has provided legal arguments on why the Windows 2000 as reported to the media (as evidenced by the cited references in the prosecution history of this application) cannot be prior art, especially if the media reports were published after the filing date of the application" (*see* Office Action dated January 10, 2007, page 3; emphasis in original). The Examiner misstates the Applicant's position, although the substance of the Examiner's statement is accurate. The Applicant has never argued that Microsoft Windows 2000 itself is not prior art: the Applicant agrees that Microsoft Windows 2000 was originally released in the year 2000, before the filing date of the patent application. But the Applicant and the Examiner disagree about what was publicly included in Microsoft Windows 2000. Reports published after the filing date of the patent application, such as "Comptech Article", are not prior art. The contents of these "reports to the media" have not been shown to describe Microsoft Windows 2000 prior to the filing date of this patent application, and the content of these "reports" cannot be used to support an assertion that Microsoft Windows 2000 renders the claims in this patent application obvious, especially where the Examiner cites to the reference as describing what was known.

The Examiner has still failed to establish that "Comptech Article" is prior art

The Examiner states that "[a]fter the Examiner establishes the date of the subject matter of the prior art, the actual publication date of the prior art does not seem to be relevant" (*see* Office Action dated January 10, 2007, page 3; emphasis in original). The Examiner appears to believe that the Applicant has acknowledged that the subject matter of "Comptech Article" is prior art before the filing date of the patent application. This conclusion is reached from the Examiner's statement that "if there is no dispute that the subject matter of the prior art is before the filing date of this application, then the actual publication date of the prior art does not seem to be relevant" (*see* Office Action dated January 10, 2007, page 3).

First, the Examiner's second statement is a conditional, as the Examiner prefaced the statement with the word "if". Thus, as the Applicant continues to dispute that "the subject matter of the prior art is before the filing date of this application", then the rest of the Examiner's statement does not matter.

Second, the Applicant disagrees with the Examiner that the "subject matter of the prior art is before the filing date of this application". The Applicant has repeatedly argued that "Comptech Article" was published after the filing date of this patent application, and as such is not prior art. Further, the Applicant respectfully points out that the Examiner has yet to establish that "Comptech Article" is prior art, within the definition of that term. The Applicant especially points out that at no time has the Applicant agreed that "Comptech Article" is proper prior art before the filing date of the patent application. Since the Examiner is relying on "Comptech Article" as the "subject matter of the prior art", the Applicant has shown that the "subject matter of the prior art" is very much in dispute.

To be proper prior art, the publication date of the reference is highly relevant. The Applicant has established a publication date of October 28, 2001 for "Comptech Article", which was after the filing date of the application, and which the Examiner has not disputed. Absent evidence that "Comptech Article" was published earlier (and more particularly, before the filing date of the patent application), "Comptech Article" is not prior art. That would mean that as "Comptech Article" is not proper prior art and is not available as a reference for a rejection, its subject matter is irrelevant, and therefore the Examiner cannot rely on "Comptech Article" as describing what was included in Microsoft Windows 2000 as of its original release date.

The Examiner appears to be arguing that Microsoft Windows 2000 is prior art to the patent application. The Applicant does not disagree with the fact that Microsoft Windows 2000 was released before the filing date of this patent application. But then the question becomes: what was included in Microsoft Windows 2000 before the filing date of the patent application?" The Examiner is relying on "Comptech Article" to answer this question. But, as argued above and previously, to use "Comptech Article" in this manner is inappropriate because "Comptech Article" is not proper prior art. "Comptech Article" is not a definitive description of the subject matter of Microsoft Windows 2000 as of its original release date. The most that can be concluded is that "Comptech Article" is a description of what one person believed Microsoft Windows 2000 included at some point on or before October 28, 2001. As discussed above and in earlier responses to Office Actions, the author could have been incorrect about his statements (and in fact pointed out the possibility of his or her error) or could have been referring to versions of Microsoft Windows 2000 that existed only after the filing date of this patent application, among other possibilities. The burden is on the Examiner to show what was

included in Microsoft Windows 2000 before the filing date of the patent application; "Comptech Article" does not satisfy that burden.

The Examiner has failed to explain why the "prior art documents" are credible

According to the Examiner:

> [T]he real question seems to be: what is the credibility of the prior art documents that have been cited in the prosecution history of this application?
>
> On this critical question, the Office decided at this time against Applicant. After an unusually difficult consideration, the Office decides at this time in favor of the credibility of the prior art documents that have been cited in the prosecution history this application.
>
> Thus, the claims are rejected.

(*see* Office Action dated January 10, 2007, pages 3-4). However, the Examiner has provided no explanation as to why the "prior art documents" are considered "credible".

Nowhere does the M.P.E.P. describe the "credibility" of prior art as a factor in making a rejection. "Credibility" appears in the M.P.E.P. only in connection with the utility of the claimed invention: if the claimed utility is not credible, that fact forms a basis for rejecting a claimed invention as lacking utility. The M.P.E.P. does not describe the "credibility" of a reference as a factor in a rejection under 35 U.S.C. §§ 102-103.

In fact, the Graham factors, recited by the Examiner, suggest that the credibility of a reference is altogether inappropriate in a rejection under 35 U.S.C. § 103(a). Credibility is a subjective interpretation of the reference: how reliable is the reference? Different people can have different opinions as to the reliability of a reference. Turning to the Graham factors, the scope and content of the prior art is an objective determination: either the reference teaches a point or it does not. Similarly, the differences between the reference and the claimed invention are an objective determination. The level of ordinary skill in the art is generally a subjective question, but has nothing to do with the reference itself. That leaves only the fourth Graham factor: the objective evidence indicating obviousness or non-obviousness. Because the fourth Graham factor requires objective evidence, a subjective interpretation such as credibility should not be used. Since the credibility of the reference does not belong in the analysis of any of the four Graham factors, the Examiner should not be arguing that the "credibility of the prior art documents that have been cited in the prosecution history of this application" (*see* Office Action

dated January 10, 2007, page 4) suggests in any way that the references should be considered as prior art.

Finally, it is worth noting that the author of "Comptech Article" explicitly recites that "Comptech Article" is not generally reliable. According to the author of "Comptech Article", "[t]his guide may have inaccuracies, use at your own risk" (*see* "The CTDP Windows 2000 Tutorial Version 0.6.1 Oct 28, 2001", http://www.comptechdoc.org/os/windows/win2k/index.html, which is the introduction to "Comptech Article"). Given that the author himself acknowledges there may be errors, the credibility of "Comptech Article" is questionable at best.

In any event, the question is not, as the Examiner suggests, the credibility of the "prior art documents". The question is their applicability: is "Comptech Article" prior art or not? This question is the initial question in determining the appropriateness of a rejection under 35 U.S.C. § 103(a). Before the Examiner can make a rejection that a claim is obvious over a reference, the reference must be "prior art". This point is established repeatedly: in 35 U.S.C. § 103(a) ("A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, *if the differences between the subject matter sought to be patented and the prior art* are such that the subject matter as a whole would have been obvious at the time the invention was made. . ."; emphasis added); in Graham v. John Deere, 383 U.S. 1, 148 U.S.P.Q. 459 (1966) ("[d]etermining the scope and contents of the *prior art*"; emphasis added); in M.P.E.P. § 2141 ("the scope and content of the *prior art* are to be determined"; emphasis added); and in M.P.E.P. § 2141.01 ("'Before answering *Graham's* "content" inquiry, *it must be known whether a patent or publication is in the prior art* under 35 U.S.C. § 102.' citing Panduit Corp. v. Dennison Mfg. Co., 810 F.2d 1561, 1568, 1 U.S.P.Q.2d 1593, 1597 (Fed. Cir.), cert. denied, 481 U.S. 1052 (1987)"; emphasis added).

Thus, "credibility" cannot enter the picture until after the documents in question are established as prior art. Whether a reference qualifies as prior art depends on the reference's availability under some section of 35 U.S.C. § 102: the subject matter of the reference and the reference's "credibility" are irrelevant. As argued repeatedly and not rebutted, "Comptech Article" is not prior art under any subsection of 35 U.S.C. § 102. As such, "Comptech Article" is not available under 35 U.S.C. § 103(a) in rejecting a claim as obvious, and the "credibility" of the reference is never reached, if it even matters at all.

The Applicant would like to remind the Examiner that in the responses to the Office Actions dated June 9, 2006 and September 21, 2006, the Applicant requested that the Examiner identify the section of 35 U.S.C. § 102 under which the Examiner believes "Comptech Article" is available as prior art. To date, the Examiner has failed to respond to this request.

The newly cited references are also not prior art

The Examiner has listed two new references on form PTO-892, attached to the Office Action dated January 10, 2007. Both of these references are from the website http://en.wikipedia.org. Neither reference has been cited in support of the rejection of the claims.

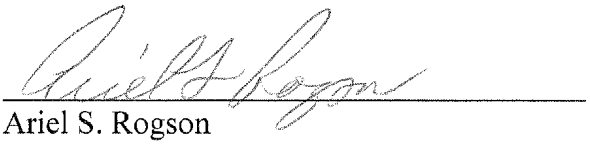
As with "Comptech Article", the Examiner has not established a publication date for either of these references. The only dates provided on these references are the dates the Examiner printed the references (January 7, 2007) and the dates the references were "last modified" (the earlier of the two being December 16, 2006). Thus, these references are not prior art any more than "Comptech Article" is prior art.

In addition, the Applicant points out that the credibility of the Wikipedia has recently been attacked. Wikipedia is "an Internet encyclopedia written entirely by volunteers" (*see* "The online credibility gap: Wikipedia article's false claim on JFK killing stirs debate", http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/12/06/WIKI.TMP&type=printable, published December 6, 2005, a copy of which is attached hereto). The volunteers who write for Wikipedia are not experts in their fields, as are authors used by encyclopedias such as Encyclopedia Britannica. In addition, persons with agendas can bias the information in Wikipedia, slanted either in favor of or against a particular position: examples of both are described in the above-referenced article. "Wikipedia lets anyone write or edit articles without having to provide credentials, prove expertise or even reveal one's name. The premise is that the system will police itself; its thousands of volunteers will weed out inaccuracies and continually improve the content" (*see* "The online credibility gap: Wikipedia article's false claim on JFK killing stirs debate", http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/12/06/WIKI.TMP&type=printable, published December 6, 2005). But there is no guarantee that, over time, articles become more accurate: this premise is entirely unproven. "[C]ritics say Wikipedia leaves the door open for anyone who wants to rewrite history . . . it's accuracy can be hard to judge" (*see* "The online credibility gap: Wikipedia

article's false claim on JFK killing stirs debate", http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/12/06/WIKI.TMP&type=printable, published December 6, 2005). In short, the articles on Wikipedia are not well authenticated. Given that the Examiner has recently focused on the credibility of references as a factor in favor of the rejection, the known unreliability of Wikipedia would make articles on Wikipedia a poor source for supporting an obviousness rejection. And even though some time has passed between the above-referenced article and the last modification of the Wikipedia references, that fact by itself does not establish the credibility of those references.

For the foregoing reasons, reconsideration and allowance of claims 1-48 of the application as amended is requested. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,
MARGER JOHNSON & McCOLLOM, P.C.



Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613
Customer No. 45842

Windows Live ID

Sign in

Windows Live ID home
Sign up
Account Services

Simplify your sign in

Create your sign in credentials (e-mail and password) once, then use them everywhere on the Windows Live ID service. You can even set the site to remember your credentials for you!

Use Windows Live ID to sign in to MSN Messenger, MSN Hotmail, MSN Music, and other sites and services! Windows Live ID works with Passport Network sites.
It's free to access Windows Live ID. After you sign up and create credentials, you can sign in on any site that displays **Microsoft Passport Network** or **Windows Live ID**.

Send instant message text to your friends with MSN Messenger, and get a free e-mail account with MSN Hotmail. Sign in to all these sites with the same e-mail and password.

If you'd like your business on the Windows Live ID service, learn how to join today.

Sign up today

Sign up for a free MSN Hotmail account
MSN Hotmail is a free e-mail service on the web. You can sign up for a free MSN Hotmail account and use your credentials to sign in to any Windows Live ID site.

- Get started now

Use an e-mail address you already have
You can use any existing e-mail address from any e-mail provider when you create your credentials for Windows Live ID. Then you can use those credentials to sign in to any Windows Live ID site.

To access e-mail at www.hotmail.com, you must use an MSN or Hotmail e-mail address, or an address associated with an MSN Personal Address.

- Get started now

Sign up for a limited account
If you don't want to use an e-mail account to access Windows Live ID, you can sign up for a limited account. Learn more about limited accounts

- Get started now

Already signed up for Windows Live ID?

If you signed in to any site or service that displays **Microsoft Passport Network** or **Windows Live ID**, then you may already have credentials for Windows Live ID sites and services. Learn how to check for an existing account

- Sign in to Account Services
- Learn more about Windows Live ID
- Report a security issue

Privacy and security

Sign in on any computer that has Internet access. Windows Live ID uses powerful online security technology and follows a comprehensive privacy policy to help protect your account information.

©2007 Microsoft Privacy | Legal | Trademarks

Sign in

Google Web Images Video News Maps more »
define:domain Search Advanced Search Preferences

Web

Related phrases: public domain domain name eminent domain domain name system domain name server top level domain domain name service domain names public domain software top-level domain

Definitions of **domain** on the Web:

- sphere: a particular environment or walk of life; "his social sphere is limited"; "it was a closed area of employment"; "he's out of my orbit"
- territory over which rule or control is exercised; "his domain extended into Europe"; "he made it the law of the land"
- the set of values of the independent variable for which a function is defined
- world: people in general; especially a distinctive group of people with some shared interest; "the Western world"
- a knowledge domain that you are interested in or are communicating about; "it was a limited domain of discourse"; "here we enter the region of opinion"; "the realm of the occult"
 wordnet.princeton.edu/perl/webwn

- Within a protein, a structural domain ("domain") is an element of overall structure that is self-stabilizing and often folds independently of the rest of the protein chain. Many domains are not unique to the protein products of one gene or one gene family but instead appear in a variety of proteins. Domains often are named and singled out because they figure prominently in the biological function of the protein they belong to; for example, the "calcium-binding domain of calmodulin. ...
 en.wikipedia.org/wiki/Domain_(protein)

- In biology, a domain or empire is the top-level grouping of organisms in scientific classification. Originally three kingdoms were distinguished: the fauna for animals, the flora (Vegetabilia) for plants, and Mineralia (early authors also treated minerals in a third kingdom). This corresponds to the old saying animal, vegetable or mineral?.
 en.wikipedia.org/wiki/Domain_(biology)

- In mathematics, the domain of a function is the set of all input values to the function.
 en.wikipedia.org/wiki/Domain_(function)

- In abstract algebra, a domain is a ring with $0 \neq 1$ such that $ab = 0$ implies that either $a = 0$ or $b = 0$. That is, it is a nontrivial ring without left or right zero divisors.
 en.wikipedia.org/wiki/Domain_(ring_theory)

- See: graphonomics
 en.wikipedia.org/wiki/Domain_(graphonomics)

- A discrete portion of a protein with its own function. The combination of domains in a single protein determines its overall function.
 www.bioinformatics.buffalo.edu/current_buffalo/glossary.html

- A region of a gene or gene product. See Gene.
 www.amfar.org/cgi-bin/iowa/bridge.html

- In air pollution modeling, the geographical area over which a simulation is performed.
 weather.gov/glossary/glossary.php

- One of the elements that comprise a DNS address. Domain names are divided into different categories: .com, .net, .org, .edu, .fr, .uk, etc.
 webmaster.lycos.co.uk/glossary/D/

- A name by which a computer connected to the Internet is identified. A typical domain name looks like this: www.ibm.com. The "www." refers to the fact that this computer is connected to the World Wide Web; the middle portion of a domain name is usually the name of the company that owns the computer—in this case,IMB ; the final portion of a domain name tells you what kind of site is served by this machine—in this case, '.com' means this is a commercial site (other types of sites are:
 www.visionsofadonai.com/onrampglossary.html

- An object, icon, or container that contains other objects representing the resources of a domain. You can use the domain object to manage those resources.
 www.sabc.co.za/manual/ibm/9agloss.htm

- A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

www.panama-hosting.com/glossary.htm

- A group of IP addresses corresponding to a specific site, group, university, or company, from which the IP address for a specific machine can be assigned.
 www.arl.org/scomm/subversive/glossary.html

- A group of computers and devices on a network that are administered as a unit with common rules and procedures and share a common name.
 www.saol.com/glossary.asp

- typically the last three letters of an Internet address represent the domain or particular section of the Internet. Major domain suffixes are listed below: .edu - Educational Institutions; .gov - US Government; .com - Commercial (business); .net - Network Infrastructure Organizations; .org - Non-profit Organizations; .mil - military organizations and country codes such as .ca for Canada, .fr for France, and .jp for Japan.
 www.library.arizona.edu/rio/glossary.htm

- The set of all first coordinates in a function.
 www.riverdeep.net/students/glossaries/algebra/Glossary.jhtml

- The domain is the part of a web address that specifies what the organisation is and where the computer is located. For example:
 www.liv.ac.uk/webteam/glossary/

- The part of the external world, including users and inmates of the system that effects and is affected by the system.
 sparc.airtime.co.uk/users/wysywig/gloss.htm

- An area under a single point of control. On the Internet there are different levels of control and each is a domain. At the lowest level is each local area network that has its own network ID. Top-level domains are .com, .org etc. In some operating systems such as NT, a domain is a group of associated computers within a LAN.
 www.micro2000uk.co.uk/network_glossary.htm

- The set from which values are selected.
 members.iinet.net.au/~lonsdale/seng/se20.htm

- A sub-set of Internet addresses. Domains are hierarchical, lower-level domains often refer to specific Web sites within a top-level domain. The distinguishing part of the address appears at the end. Example of top-level domains: .com, .edu, .gov, .org (subdividing addresses into areas of use). There are also numerous geographic top-level domains: .ar, .ca, .fr, .ro (referring to specific countries).
 www.virtechseo.com/seoglossary.htm

- synonyms: materials, object, situation. analog: subject matter
 www.geocities.com/Athens/Delphi/5179/Glossary.htm

- A domain is the part of the Uniform Resource Locator (URL) that locates an organization or entity on the Internet; for example, www.watchfire.com.
 webxact.watchfire.com/themes/standard-en-us/help/glossary.html

- In a database, the set of allowed values for a table column, for example all positive integers.
 www.geog.leeds.ac.uk/staff/m.blake/magis/glossary/esriglos.htm

- as well as its common overseas uses can mean a public park, especially a small flat grassed area within urban surroundings (from demesne: any estate in land).
 www.nationmaster.com/encyclopedia/New-Zealand-English

- For DNS, a group of workstations and servers that share a single group name.
 www.wrightcolorgraphics.com/d.htm

- The address of a site, without the protocol, path, page or other items attached. For example, microsoft.com is a domain, however, a full URL could be http://www.microsoft.com/stuff/page.html.
 www.netefxnw.com/internet_terminology.htm

- A Domain is defined as the physical computer on which the GroupDrive Server Service is running. The GroupDrive Administrator program can connect to the Local Domain. For each Domain, you can define zero or more Server instances. Each Server instance is identified by a unique IP/Port combination. In the graphic at the right, the domains are represented by the blue computer monitor located directly under the Domains node in the tree.
 www.groupdrive.com/support/groupdrive/webhelp/terminology.htm

- Part of the DNS (domain naming system) name that specific details about the host. A domain is the main subdivision of Internet addresses, the last three letters after the final dot, and it tells you what kind of organization you are dealing with. There aresix top level domains widely used in the US : .com (commercial), .edu (education), .et (network operations), .gov (US government),

.mil (US military), .org (organization). Other, two-letter domains represent countries, thus, ...
www.expedite-email-marketing.com/internet_marketing_glossary_internetmarketingtermsdefinition.htm

- This is the geographic area of study around LANL in which risk estimates are made.
www.racteam.com/LANLRisk/Glossary.htm

Find definitions of **domain** in: Chinese (Simplified) Chinese (Traditional) Dutch **English** French German Italian Portuguese Russian Spanish all languages

define:domain Search

Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

©2007 Google



Frequently Asked Questions

- **Using Windows Update**
- **Supported versions and languages**
- **Troubleshooting**
- **Networking and Advanced Information**

Using Windows Update

What is Windows Update?
A Microsoft Web site that provides updates for Windows operating system software and Windows-based hardware. Updates address known issues and help protect against known security threats.

Tip:

- If you turn on Automatic Updates, Windows Update can deliver high priority updates to your computer as they become available. You can decide when and how updates are installed.

How does it work?
When you visit the Web site, Windows Update scans your computer and tells you which updates apply to your software and hardware. You choose the updates that you want to install and how to install them.

What types of updates can I get?
Microsoft releases many types of updates that address a broad range of issues. To make it easier for you to get the most important updates—updates that help protect your computer and your information—Windows Update uses these categories:

- **High priority**
 Critical updates, security updates, service packs, and update rollups that should be installed as soon as they become available and before you install any other updates.
- **Software (optional)**
 Non-critical fixes for Windows programs, such as Windows Media® Player and Windows Journal Viewer 1.5.
- **Hardware (optional)**
 Non-critical fixes for drivers and other hardware devices, such as video cards, sound cards, scanners, printers, and cameras.

What's the difference between Express and Custom?

- **Express (recommended)** displays all high priority updates for your computer so that you can install them with one click. This is the quickest and easiest way to keep your computer up to date.
- **Custom** displays high priority and optional updates for your computer. You review and select the updates that you want to install, one by one.

Do I need to install optional updates?
No. Optional updates address minor issues or add non-critical functionality to your computer. It is more important to install high priority updates so that your computer gets the latest critical and security-related software.

Can I get updates automatically?
Yes, if you turn on **Automatic Updates**. Windows will check for the latest high priority updates for your computer and install them according to your Automatic Updates setting.

Is Automatic Updates the same as Windows Update?
Yes, but Automatic Updates delivers only high priority updates. To get optional updates, you still need to visit the Windows Update Web site.

What is Automatic Updates?
It's a feature that works with Windows Update to deliver critical and security-related updates as they become available. When you turn on Automatic Updates (recommended), Windows automatically looks for high priority updates for your computer. You decide how and when the updates are installed.

How can I get more information about an update before I install it?

Click the name of each update to view its description. To view system requirements and support information, click the **Details** link provided in each description.

Do I have to do anything to install an update?
Sometimes. Some updates require you to accept an End User License Agreement (EULA), answer a question about the installation process, or restart your computer before you can install them.

What happens if I select "Don't show me this update again"?
Windows Update will no longer ask you to review or install that update. However, if you hide a high priority update, you might be reminded that you're missing an update that is critical to the security of your computer.

If I hide an update, how do I get it back later?
On the Windows Update Web site, click **Restore hidden updates**, and then review and install the updates that you want.

How often does Windows Update release new updates?
Security-related updates are released once a month. However, if a security threat occurs, such as a widespread virus or worm that affects Windows-based computers, Microsoft will release a corresponding update as soon as possible.

Other types of updates are released whenever they are ready. It's a good idea to turn on Automatic Updates so that your computer can receive high priority updates as they become available.

How do I add Windows Update to my list of trusted Web sites?

- In Internet Explorer, on the **Tools** menu, click **Internet Options**.
- On the **Security** tab, click **Trusted Sites**, and then click **Sites**.
- Under **Add this Web site to the zone**, type (or copy and paste) this URL: http://update.microsoft.com/windowsupdate/.
- Click **Add**, and then click **OK**.

Supported versions and languages

Which operating systems does Windows Update support?
The Windows Update website offers updates for Windows operating systems only.

Operating System Version	Windows Update Support
Windows Server 2003	
• Windows Server 2003 with Service Pack 1	• Ongoing
• Windows Server 2003	• No new updates offered after June 2007
Windows XP	
• Windows XP with Service Pack 2	• Ongoing
• Windows XP with Service Pack 1	• No new updates offered after September 2006; previous updates available
• Windows XP	• No new updates offered after September 2004; previous updates available
Windows 2000	
• Windows 2000 with Service Pack 4	• Ongoing
• Windows 2000 with Service Pack 3	• No new updates offered after June 2005; previous updates available
• Windows 2000 with Service Pack 2	• No new updates offered after June 2004; previous updates available

• Windows 2000 with Service Pack 1	• No new updates offered after August 2004; previous updates available
• Windows 2000	• No longer supported
Additional operating systems	
• Windows Millennium Edition	• Critical and security updates only after December 2003; no updates will be offered after June 2006
• Windows 98	• Critical and security updates only after August 2002; no updates will be offered after June 2006
• Windows NT Server	• No longer supported after December 2004
• Windows NT Workstation	• No longer supported after June 2004

Tip: Not sure which version of Windows your computer is running? Visit the Microsoft Protect Your PC website and, under Getting Started, click **Find out which version of Windows your computer is using.**

How long will I receive updates and support for my product?
For information about how long Microsoft products are supported, see the current Microsoft Support Lifecycle Policy.

Which browser versions can I use to access Windows Update?
You can use Microsoft Internet Explorer 5 but we recommend using Internet Explorer 6 or later.

How do I know which version of Internet Explorer I'm using?
In Internet Explorer, on the **Help** menu, click **About Internet Explorer.**

Can I view the Windows Update Web site using another language?
Yes, but updates will no longer appear in the same language that you use to view links, options, and instructions on the Web site. Titles and details for an update are displayed using your computer's default language.

How do I change my language settings?

- On the Windows Update Web site, click **Change settings**.
- Select the language that you want to use to view Windows Update, and then click **Apply changes now**.
- When you are asked to confirm the change, do one of the following:
 - To change your language settings immediately, click **OK**.
 (You will need to review and select updates again.)
 - To use the new language after installing any updates that you've selected, click **Cancel**.
 (The next time you visit Windows Update, your new language setting will be applied.)

Why does Windows Update recommend a language for me to use?
It matches the default language setting for your computer. If you use it, you can view the Web site using the same language as the titles and details of any updates that apply to your computer.

Can I get updates in multiple languages?
Yes. Windows Update automatically detects language settings for each program on your computer. If you use multiple languages, you will be offered updates for each program in the appropriate language.

Troubleshooting

What happens if I cancel the download process or disconnect from the Internet before an update is fully downloaded?
The next time you connect to the Internet, the update will continue to download from the point at which it was interrupted.

I get an Internet Explorer error—how do I change my settings to work with Windows Update?
Use the default security settings:

- In Internet Explorer, on the **Tools** menu, click **Internet Options**.
- On the **Security** tab, click **Internet zone**, and then click **Default Level**.

To prevent problems, you can also add Windows Update to your list of trusted sites (instructions provided in the Using Windows Update section).

I get ActiveX or scripting warnings when I use Windows Update—is there a problem?
No. Windows Update uses these technologies to determine which updates your computer needs. As a security measure, Windows Update ActiveX controls are digitally signed by Microsoft. But attackers sometimes use the same technologies to harm your computer. Internet Explorer warns you so that you can decide whether or not to trust Web sites that use these controls.

Get more information about digital certificates, trusting Web sites, and choosing security settings by searching Internet Explorer Help. (If you don't want to see warnings when you use Windows Update, you can change your security settings but it's not recommended. If you lower the level of your settings, your computer is more vulnerable to viruses and other security threats.)

Why can't I view update details, installation history details, or troubleshooting articles?
Your pop-up blocking software or settings do not allow you to open new browser windows from links that you click within a Web site.

To change Pop-up Blocker settings (available for Internet Explorer 6 on Windows XP SP2 or later):

- In Internet Explorer, on the **Tools** menu, point to **Pop-up Blocker**, and then click **Pop-up Blocker Settings**.
- Do one of the following:
 - To allow pop-up windows only when using Windows Update, under **Address of Web site to allow**, type (or copy and paste) this URL: https://update.microsoft.com and then click **Add**.
 - To allow new browser windows to open when using any secured (https://) Web sites, in the **Filter Level** list, click **Low: Allow pop-ups from secure sites**.

If you use other pop-up blocking software, find out whether you can change your settings just for links that you click within a Web site. If not, you might need to allow pop-ups while using Windows Update.

Where do I go if I have problems installing an update?
See Windows Update Help and Support for information about these and other options:

- Windows Update Troubleshooter
- Windows Update Support Center
- Windows Update Newsgroup
- Microsoft Online Assisted Support (no-cost for Windows Update issues)

Why can't I find an update after I've restored hidden updates?
Another update that you've installed has already addressed the same issue. For example, if you install a service pack or update rollup, your computer might no longer need the update that you'd previously hidden.

Why can't I install some updates at the same time as other updates?
Some updates, such as service packs and update rollups, include several updates or address the same issues.

Other types of updates require you to restart your computer before they can take effect. You must install these updates separately. You can then return to Windows Update to see if more updates apply.

Networking and Advanced Information

What if I need to update more than one computer?
If you have a home or small office network, you need to update each computer individually.

If you are a network administrator, go to Administrator options for information about additional update services, such as the Windows Update Catalog and Windows Server Update Services.

What is Microsoft Baseline Security Analyzer (MBSA)?
MBSA is a tool that scans networked, Windows-based computers for common security misconfigurations and missing security

updates. It includes a graphical and command-line interface, and can perform local or remote scans. It can also generate a security report for each computer in a network that it scans. For more information, read the Microsoft Baseline Security Analyzer overview.

What is Windows Server Update Services?
Windows Server Update Services, previously known as Software Update Services (SUS), is the update management component for the Windows Server 2003 family. It scans and reports security settings for all computers within a network, and synchronizes updates. It also helps reduce risks and costs commonly associated with updating medium to large networks. For more information, visit the Windows Server System site for Windows Server Update Services.

Which types of updates do Automatic Updates, Windows Update, and Windows Server Update Services deliver?

	Automatic Updates	Windows Update Web Site		Windows Server Update Services*
		Express	**Custom**	
High priority Updates				
Critical Updates	X	X	X	X
Security Patches	X	X	X	X
Update Rollups	X	X	X	X
Service Packs	X	X	X	X
Optional Updates				
Software			X	X
Hardware			X	
Beta software			Opt-in setting	

*Network administrators can select any or all supported updates to distribute. Updates for Microsoft products such as Office, SQL Server and Exchange Server will be made available for use with Windows Server Update Services servers (but not for use with Software Update Services (SUS) 1.0 or SUS 1.0 with Service Pack 1 servers).

How can I get more updates, or updates that Windows Update doesn't offer?
Visit the following Web sites:

- Microsoft Download Center
 Get downloads for Microsoft products. Downloads are available in over 70 languages.
- Windows Update Catalog
 Search for updates for servers and other computers using Windows operating systems.
- Microsoft Office Online
 Find updates for the Microsoft Office System, versions 97, 98 and later. Downloads include templates, assistance content, and clip art.
- Microsoft Premier Support
 Learn about Premier Support benefits, including additional updates, such as pre-release software.

Random Small Primes

10 to 100 digits (page 1 of 3)

Here is a frequently asked question at the Prime Pages:

> I am working on a project for which I need some primes that are, say, 10 - 100 digits long, so the table that you have posted one the web is an overkill for me. Could you, please, tell me where I might go for those?

Below I give some small primes. Obviously these should not be used for cryptological uses which rely on the secrecy of the prime factors of a modulus (as they have been published here) but they will suffice for testing algorithms... I started with a string of "random" digits (created using UBASIC's irnd() function), checked for small prime divisors, and if there were none, I used APRT-CL for the primality proof.

Digits: 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, (larger).

Ten random 10 digit primes

- 5915587277
- 1500450271
- 3267000013
- 5754853343
- 4093082899
- 9576890767
- 3628273133
- 2860486313
- 5463458053
- 3367900313

Ten random 20 digit primes

- 48112959837082048697
- 54673257461630679457
- 29497513910652490397
- 40206835204840513073
- 12764787846358441471
- 71755440315342536873
- 45095080578985454453
- 27542476619900900873
- 66405897020462343733
- 36413321723440003717

Ten random 30 digit primes

- 671998030559713968361666935769
- 28217448859959950057384998O909
- 52141962285665768942387261377l
- 36273603587051533112852733O659
- 11575698666830365789896246795 7
- 59087261282517955133610219659 3
- 56481966994673551244454355650 7
- 51382121702412924394841105680 3
- 41606470020165830619632013793 1
- 28082936986213471939003661706 7

Ten random 40 digit primes

- 2425967623052370772757633156976982469681

- 145173047051377849223662959899216603506 7
- 607538052934545886014457739870476161464 9
- 361541588158511790855024350530978552623 1
- 599283023552414275838685063377325868111 9
- 438416518286724058480593097095157501369 7
- 599181055463339651776702496758089432115 3
- 684794468203744468116277067279828891384 9
- 414616291945853016895335728220162112405 7
- 557037327018318166509805248110967898941 1

Ten random 50 digit primes

- 22953686867719691230002707821868552601124472329079
- 30762542250301270692051460539586166927291732754961
- 29927402397991286489627837734179186385188296382227
- 46484729803540183101830167875623788794533441216779
- 95647806479275528135733781266203904794419563064407
- 64495327731887693539738558691066839103388567300449
- 58645563317564309847334478714939069495243200674793
- 48705091355238882778842909230056712140813460157899
- 15452417011775787851951047309563159388840946309807
- 53542885039615245271174355315623704334284773568199

Ten random 60 digit primes

- 62228809749892649614109586926888399956309606359249805529046 1
- 61069253327050875044193122638420985640587665799399754717138 7
- 66848605169669119010289530642699937039405481750691662900185 1
- 31353958997402666638501031970734176101289470405573395248411 3
- 47028778585807644156672350786675109292701582483488190676350 7
- 36172091281075540821570846064584285972271586520681623794458 7
- 37834891023346564785918442133461553254374974718532163408621 9
- 66948310657809240593656083101755615462290195004890301665128 9
- 35130003395868365662928119743023695104507791707422777883480 7
- 51170437494691749063885110491246228414424081312507145412615 1

Ten random 70 digit primes

- 46695238499321305088763925547134075213191172396379432249800156761564 91
- 49062754277678023583577037309380873621761426426990938279331078882537 09
- 24091307818949865719567777216499688015114659154511963762691773050668 67
- 75950091510800166524492237927267489854520529454131600736458420908277 11
- 38225356320335094642661598118051978548720670429907160058083721946649 33
- 58859039651805866690735493606448005834581382380120336475396497350172 87
- 58507257027668292914913707121362860099486421251314361133428157864445 67
- 42370809798686077427508086008466383180228635931477747395564279432949 37
- 37731808162193846067841895388995531104994422957825767022222803849175 51
- 95478480651537733357074958854535661200691302702467688067907083939099 99

Ten random 80 digit primes

- 18532395500947174450709383384936679868383424444311405679463280782405796233163977
- 39688644836832882526173831577536117815818454437810437210221644553381995813014959
- 44822481511601066098713481453161748979849764719554039096395688045048053310178487
- 54875133386847519273109693154204970395475080920935355580245252923343305939004903
- 40979218404449071854385509743772465043384063785613460568705289173181846900181503
- 56181069873486948735852120493417527485226565150317825065106074926567306630125961
- 19469495355310348270990592580191998639221450743640952620236903851789700309402857
- 34263233064835421125264776608163440537925705997962346596977803462033841059628723

- 14759984361802021245410475928101669395348791811705709117374129427051861355011151
- 671203333685202725329406691122280254749705789380462806183943715514889883237942 43

Ten random 90 digit primes

- 282755483533707287054752184321121345766861480697448703443857012153264407439766013042402571
- 370332600450952648802345609908335058273399487356359263038584017827194636172568988257769601
- 463199005416013829210323411514132845972525641604435693287586851332821637442813833942427923
- 374413471625854958269706803072259202131399386829497836277471117216044734280924224462969371
- 664869143773196608462001772779382650311673568542237852546715913135688434614731717844868261
- 309133826845331278722882330592890120369379620942948199356542318795450228858357445635314757
- 976522637021306403150551933319006137720124048624544172072735055780411834104862667155922841
- 635752334942676003169313626814655695963315290125751655287486460091602385142405742365191277
- 625161793954624746211679299331621567931369768944205635791355694727774487677706013842058779
- 204005728266090048777253207241416669051476369216501266754813821619984472224780876488344279

Ten random 100 digit primes

- 2074722246773485207821695222107608587480996474721117292752992589912196684750549658310084416732550077
- 2367495770217142995264827948666809233066409497699870112003149352380375124855230068487109373226251983
- 1814159566819970307982681716822107016038920170504391457462563485198126916735167260215619523429714031
- 5371393606024775251256550436773565977406724269152942136415762782810562554131599074907426010737503501
- 6513516734600035718300327211250928237178281758494417357560086828416863929270451437126021949850746381
- 5628290459057877291809182450381238927697314822133923421169378062922140081498734424133112032854812293
- 2908511952812557872434704820397229928450530253990158990550731991011846571635621025786879881561814989
- 2193992993218604310884461864618001945131790925282531768679169054389241527895222169476723691605898517
- 5202642720986189087034837832337828472969800910926501361967872059486045713145450116712488685004691423
- 7212610147295474909544523785043492409969382148186765460082500085393519556525921455588705423020751421

Another prime page by *Chris Caldwell*

SFGate.com

The online credibility gap

Wikipedia article's false claim on JFK killing stirs debate

Carolyn Said, Chronicle Staff Writer
Tuesday, December 6, 2005



What if an online encyclopedia read by millions said you shot JFK?

Wikipedia, an Internet encyclopedia written entirely by volunteers, claimed that a prominent journalist might have been involved in the assassinations of the Kennedy brothers, a false charge that has highlighted the Achilles' heel of such do-it-yourself Web sites.

The journalist, John Seigenthaler Sr., 78 -- who was an administrative assistant to Robert Kennedy as well as one of his pallbearers -- wrote an op-ed piece in USA Today last week protesting the "false, malicious" story.

"Wikipedia is a flawed and irresponsible research tool," Seigenthaler wrote.

Wikipedia removed the allegation in early October, more than four months after it was first posted.

The communally produced compendium has become an accepted source of information for millions of Web surfers. With 2.5 billion page views a month, it is the second-most visited reference site on the Web (after Dictionary.com), according to Hitwise.

But critics say Wikipedia leaves the door open for anyone who wants to rewrite history, whether it's your neighbor with a grudge, a nut job floating a conspiracy theory or someone repeating an urban legend. As with other Web sources such as blogs, its accuracy can be hard to judge.

In another recent incident, former MTV video jockey Adam Curry was accused of editing Wikipedia's entry on podcasting to inflate his role in its creation and take credit away from other people. Curry said he was simply trying to ensure the article's accuracy.

Wikipedia lets anyone write or edit articles without having to provide credentials, prove expertise or even reveal one's name. The premise is that the system will police itself; its thousands of volunteers will weed out inaccuracies and continually improve the content. This week, Wikipedia said it would modify its rules so only registered users can post new entries. Users can become registered with a 20-second signup that does not require an e-mail address. Anyone, registered or not, can still edit any article. In January the site will add a way for users to give feedback on Wikipedia articles.

Founder Jimmy Wales said the changes hadn't been made in response to the Seigenthaler incident but were "fortuitously timed."

Wales, 39, retired as a futures and options trader with enough resources to "support himself and his wife for the rest of their lives," according to a Wired article quoted in the Wikipedia entry on him.

In an interview, Wales said he started had Wikipedia in 2001 as a way to "hearken back to the early dream of the Internet; let's get people together; let's share knowledge."

The name came from wiki wiki, a Hawaiian expression for quick, combined with encyclopedia. On the Internet, wiki now describes any communally created Web site or page.

"The big-picture vision was to give away a free encyclopedia to every person on the planet in their own language," Wales said. While Wikipedia's English version, with over 840,000 articles, is its largest, the site offers entries in 82 languages.

That ambitious goal is linked to modest capital expenditures. Wikipedia, based in St. Petersburg, Fla., has only three paid staffers; Wales volunteers his time. Its annual budget of less than $2 million, raised from donations, goes primarily for servers to house its burgeoning collection of information.

Wales acknowledges that the Seigenthaler incident shows Wikipedia isn't perfect but says it is "pretty good and getting better" at policing itself. In fact, as it matures, he thinks its accuracy will surpass that of the Encyclopedia Britannica.

"It's a mistake to think about Britannica's content as being vetted while ours isn't," he said. "In the future, people will look at an article from Britannica and say, 'This was written by two people and reviewed by two more; I want an article reviewed by hundreds of people, fact-checked scrupulously by dozens and dozens of people.' In the future, we can say Britannica can't touch these (Wikipedia's) articles; it doesn't have the manpower to do it."

But many devotees of traditional research tools think there's a danger in relying on the accuracy of an open-source encyclopedia.

"If you look at the Encyclopedia Britannica, you can be fairly sure that somebody writing an article is an acknowledged expert in that field, and you can take his or her words as being at least a scholarly point of view," said Michael Gorman, president of the American Library Association and dean of library services at Cal State Fresno. "The problem with an online encyclopedia created by anybody is that you have no idea whether you are reading an established person in the field or somebody with an ax to grind. For all I know, Wikipedia may contain articles of great scholarly value. The question is, how do you choose between those and the other kind?"

Gorman thinks the answer for academia lies in encouraging students to think critically. "Anyone involved in higher education will tell you one of the biggest problems is uncritical acceptance (by students) of anything that's online," he said.

Pamela Samuelson, a professor of law and information management at UC Berkeley, says Wikipedia shows how the role of the editorial process is now up for grabs.

"The old phenomenon of the encyclopedia was that you have editors, and the job of the editors is to commission very thoughtful and accurate pieces by people who really know what they're talking about, and then you compile the information together, and everybody buys it because it's the definitive thing," she said.

Samuelson said the recent Wikipedia incident underscored the need for a way to authenticate its information.

"Like many people who grew up with 'old media,' I like the authoritativeness of a lot of resources that I continue to rely on," she said. "I do worry that as more and more things become available only online that we need some new devices to deal with authoritativeness issues. I want to be able to have clarity on how much I can rely on certain kinds of resources. I think that more of these checks and balances will emerge."

Wales says Wikipedia does have many systems to help monitor and improve accuracy. Each Wikipedia article includes extensive links to original source material, a "talk" page to discuss it and a history of how it's been changed. In a "very social process," its users continually chat about articles online, he says. Frequent users' comments have more credence, Wales says. In October, Wikipedia had 1,854 users who made at least 100 edits to its English pages and 43,531 who made at least 10 edits.

The Communications Decency Act, which Congress passed in 1996, shields Internet service providers like Wikipedia from liability for the content they carry. So even people who were defamed, like Seigenthaler, cannot sue the site. Seigenthaler wrote in USA Today that he couldn't track down the author of the false accusation against him without a subpoena to the person's Internet provider.

"This legal immunity is critical to give forums the space necessary to allow others to speak," said Kurt Opsahl, a staff attorney with the Electronic Frontier Foundation. "It's simply impossible for Wikipedia to review every post before it is made, so if you had any rule other than immunity for those posts, projects like Wikipedia would be in danger. I think Wikipedia is working hard to refine its process. Its core argument is that the sum of everybody's knowledge will tend toward the truth over time."

http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/12/06/WIKI.TMP

This article appeared on page **A - 1** of the San Francisco Chronicle

San Francisco Chronicle Sections Go

© 2005 Hearst Communications Inc. | Privacy Policy | Feedback | RSS Feeds | FAQ | Site Index | Contact